Вариант 9

Зашифрованное сообщение	ю к й й и б ц б
Ключ	Диск на рис. 9

Вариант 10

Зашифрованное сообщение	ю л к ю к щ е з
Ключ	Диск на рис. 9

Шифр Виженера

Шифр Виженера – это полиалфавитный шифр, который использует таблицу ключей для замены каждой буквы открытого текста на соответствующую букву зашифрованного текста. Таблица ключей состоит из последовательности алфавитов, и каждый алфавит используется для шифрования одного символа открытого текста.

Суть алгоритма шифрования проста. Шифр Виженера — это последовательность шифров Цезаря с различными значениями сдвига (ROTX — см. Шифр Цезаря). То есть к первой букве текста применяется преобразование, например, ROT5, ко второй, например, ROT17, и так далее. Последовательность применяемых преобразований определяется ключевой фразой, в которой каждая буква слова обозначает требуемый сдвиг, например, фраза ГДЕ ОН задает такую последовательность шифров Цезаря: ROT3-ROT4-ROT5-ROT15-ROT14, которая повторяется, пока не будет зашифрован весь текст сообщения. Так же используют таблицу Виженера.

	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а
б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б
в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в
г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г
д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д
е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е
ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё
ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж
з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и
й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й
к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л
м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м
н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н
о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о
п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р
с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с
т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т
у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ
ы	ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы
ь	э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь
э	ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
ю	я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю
я	а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я

Рисунок 11. Таблица Виженера

Пример: Необходимо зашифровать сообщение "МИРЭА", используя ключ “ЗИМА”. Так как ключ меньше исходного сообщения, то он записывается несколько раз.

Таблица 13. Пример шифрования

Исходный текст	МИРЭА
Ключ	ЗИМАЗ
Зашифрованное сообщение	хтююи

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	рогыыт
Ключ	Лето

Вариант 2

Зашифрованное сообщение	мэнойфа
Ключ	осень

Вариант 3

Зашифрованное сообщение	лудбйхще
Ключ	весна

Вариант 4

Зашифрованное сообщение	ушърезаёщ
Ключ	зима

Вариант 5

Зашифрованное сообщение	цйцрнтл
Ключ	киб

Вариант 6

Зашифрованное сообщение	псоянёбрхё
Ключ	день

Вариант 7

Зашифрованное сообщение	фгщржъш
Ключ	жук

Вариант 8

Зашифрованное сообщение	бфдвгюёён
Ключ	ночь

Вариант 9

Зашифрованное сообщение	вёгтща
Ключ	пара

Вариант 10

Зашифрованное сообщение	яомбтйл
Ключ	мышь

Шифр Трисемуса

Шифр Трисемуса – это один из самых известных шифров, который был разработан в XVI веке. Он использует замену букв на другие буквы или символы с помощью ключа. Для дешифровки сообщения нужно знать ключ, который использовался при шифровании.

В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием "Полиграфия". В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. При шифровании находят в этой таблице очередную букву открытого текста и записывают в шифртекст букву, расположенную ниже неё в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самая верхнюю букву из того же столбца.

Исходное сообщение: РТУМИРЭА

Ключ РТУ

Таблица 14. Таблица для шифрования с ключом РТУ

Р	Т	У	А	Б	В
Г	Д	Е	Ё	Ж	З
И	Й	К	Л	М	Н
О	П	С	Ф	Х	Ц
Ч	Ш	Щ	Ъ	Ы	Ь
Э	Ю	Я	1	2	3

Зашифрованное сообщение: ГДЕХОГРЁ

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	ЧДЩДХ С ЕДВОЭП; МПОГ ЮЬМПЕОЗЦ
Ключ	уникальность

Вариант 2

Зашифрованное сообщение	ШД МДЩДЙП ХСЧОПЦ, ЕТЬЮОДЦ
Ключ	уникальность

Вариант 3

Зашифрованное сообщение	ЬФ ЩПФП ЕДВОЗЯТД ЖВСЕЁБВД
Ключ	уникальность

Вариант 4

Зашифрованное сообщение	ЁЩС МПЗСЭ3 ШДМ ДТОДЧ
Ключ	уникальность

Вариант 5

Зашифрованное сообщение	ЮПЩПЧЬЫБ МЬЯЁЕЁБИ Е ЗПЕОДН ЩБЕЭЗПВБ
Ключ	уникальность

Вариант 6

Зашифрованное сообщение	ИДЖМНС ЧФЗФС ЧЦНМР ШФДХ2 ЧТКШНУУФС
Ключ	Ёлка

Вариант 7

Зашифрованное сообщение	НЧШ3 Щ ТНУК ЮНЧШГЦЕЖ ЧДЩЙ
Ключ	Ёлка

Вариант 8

Зашифрованное сообщение	УЖ ЗНЦНЙЩ ХЩЧШ2УУ2Ы ИФДУ
Ключ	Ёлка

Вариант 9

Зашифрованное сообщение	ЙФЦРШ Р ЕЦЩОРШЧК ХДЖУНШЖ
Ключ	Ёлка

Вариант 10

Зашифрованное сообщение	НЧШ3 ОНУЯРУ2 И ЦЩЧЧЕРЫ ЧНДНУ3КЫ
Ключ	Ёлка

Решётка Кардано

Решётка Кардано – исторически первая известная шифровальная решётка, трафарет, применявшийся для шифрования и дешифрования, выполненный в форме прямоугольной (чаще всего – квадратной) таблицы-карточки, часть ячеек которых вырезана, и через которые наносился шифротекст. Пустые поля текста заполнялись другим текстом для маскировки сообщений под обычные послания – таким образом, применение решётки является одной из форм стеганографии.

Шифратор помещает решетку на лист бумаги и пишет сообщение в прямоугольных отверстиях, в которых помещается отдельный символ, слог или целое слово. Исходное сообщение оказывается разделенным на большое число маленьких фрагментов.

Одна из разновидностей решетки Кардано – вращающаяся решетка или сетка.

Вращающиеся решетки бывают квадратными и прямоугольными.

Чтобы зашифровать текст таким образом, необходимо приложить решетку к листу бумаги и вписать текст сообщения в вырезанные ячейки, затем повернуть решетку по часовой стрелке (или по часовой) и продолжить запись сообщения, потом снова повернуть решетку и т.д.

Исходное сообщение: Университет РТУМИРЭА ! будет зашифровано на поле, которое представлено на рис. 12.

В примере решетки Кордано имеет 10 открытых областей (рис. 12), а сообщение 20 символов, следовательно, для шифрования сообщения понадобится повернуть решётку, в примере будет разобран поворот против часовой стрелке.

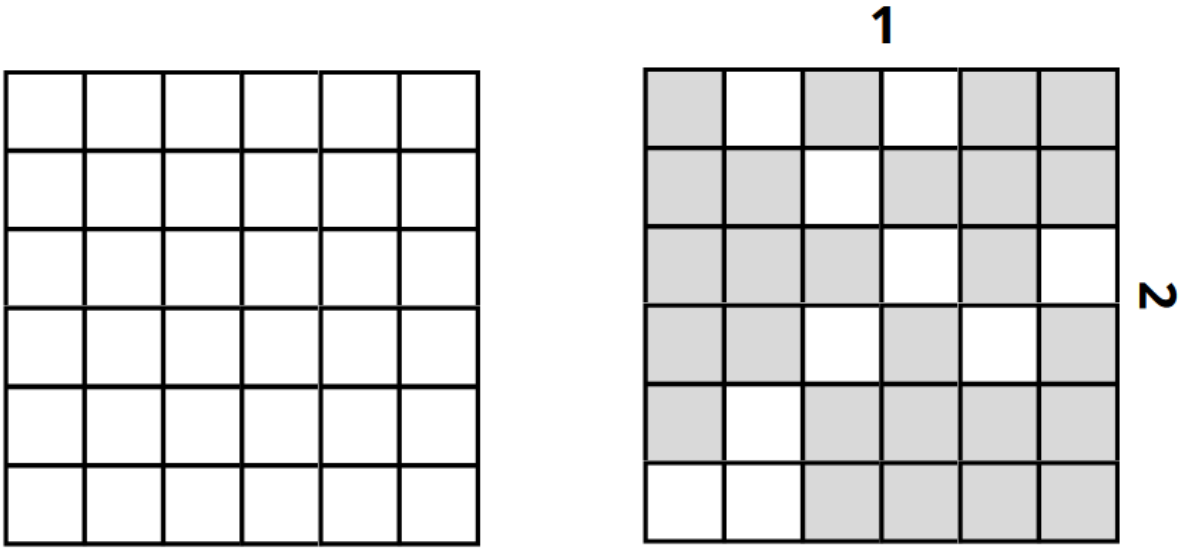

Рисунок 12. Поле и решетка для шифрования

Порядок шифрования:

1) сопоставить поле и решетку (положение 1) и нанести 10 символов исходного текста (рис. 13);

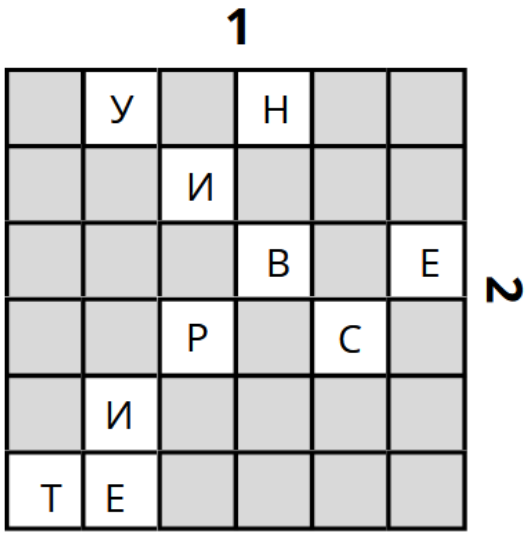

Рисунок 13. Шифрование 10 символов

2) на рис. 14 представлено поле после первого этапа шифрования;

Рисунок 14. Поле после шифрования 10 символов

3) сопоставить поле и решетку (положение 2, те есть повернуть решетку относительно исходного состояния против часовой) и нанести еще 10 символов исходного текста (рис. 15);

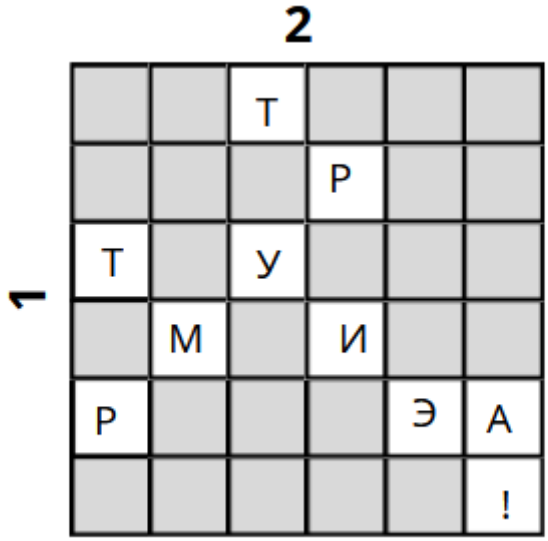

Рисунок 15. Шифрование следующих 10 символов

4) после шифрования получено поле на рис. 16;

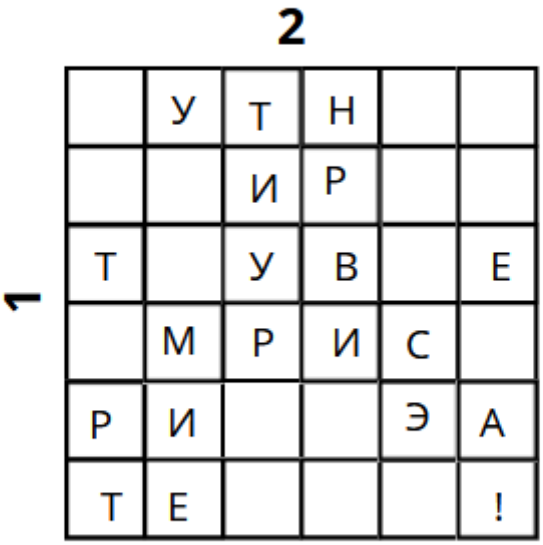

Рисунок 16. Поле после шифрования 20 символов

5) далее случайным образом необходимо заполнить поле буквами алфавита (рис. 17);

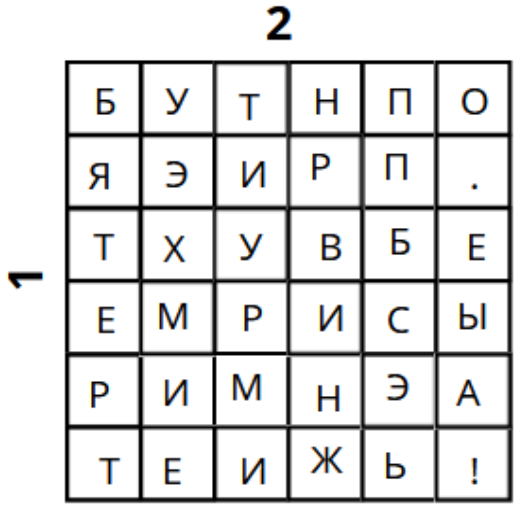

Рисунок 17. Заполненное поле после шифрования

6) таким образом удалось зашифровать исходное сообщение.

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Ключ	Размер поля 6х6, решетка – рис. 12
Зашифрованное сообщение	цкоотхусрвчсиллодчосеяседтщйенанавгь

Вариант 2

Ключ	Размер поля 6х6, решетка – рис. 12
Зашифрованное сообщение	ыдуонтпевчяянеаомлояьпнеоосбраскхщшк

Вариант 3

Ключ	Размер поля 6х6, решетка – рис. 12
Зашифрованное сообщение	щкваыцзмккрпкяенеадкваыкрсмутнтасчсн

Вариант 4

Ключ	Размер поля 6х6, решетка – рис. 12
Зашифрованное сообщение	нвлсишчъеоьпгйрршдеуцсефтсптнетаубве

Вариант 5

Ключ	Размер поля 6х6, решетка – рис. 12
Зашифрованное сообщение	тляеарбупчляичхекшапеокпегресторсчсь

Вариант 6

Ключ	Размер поля 6х6, решетка – рис. 12
Зашифрованное сообщение	кбьуаппарететлияьсозвненутлатрабсхсн

Вариант 7

Ключ	Размер поля 6х6, решетка – рис. 12
Зашифрованное сообщение	езквзщсцеабъюетззднсыосшчвбсьюеряимич

Вариант 8

Ключ	Размер поля 6х6, решетка – рис. 12
Зашифрованное сообщение	овоельтасбрцнаонжапввдртееорнимячеря

Вариант 9

Ключ	Размер поля 6х6, решетка – рис. 12
Зашифрованное сообщение	Алпеобритеьлчуаот-отпловерфтниавйищй

Вариант 10

Ключ	Размер поля 6х6, решетка – рис. 12
Зашифрованное сообщение	Аоясбуцзеражоумнтьба-нвртревикемэпки

Шифр Бэкона

Шифр Бэкона (или «двухлитерный шифр») – метод сокрытия секретного сообщения, придуманный Фрэнсисом Бэконом в начале XVII века. Он разрабатывал шифры, которые бы позволяли передавать секретные сообщения в обычных текстах так, чтобы никто не знал об этих сообщениях. Шифр базируется на двоичном кодировании алфавита символами «А» и «В», которым

можно сопоставить «0» и «1». Затем секретное послание «прячется» в открытом тексте с помощью одного из способов сокрытия сообщений

Методы кодирования

Для кодирования сообщений Фрэнсис Бэкон предложил каждую букву текста заменять на группу из пяти символов «A» или «B» (так как последовательностью из пяти двоичных символов можно закодировать $2^5 = 32$ символа, что достаточно для шифрования 26 букв английского алфавита). Это можно сделать несколькими способами:

Алфавитный метод

Во времена Фрэнсиса Бэкона английский алфавит состоял из 24 букв ввиду того, что буквы «I» и «J», а также «U» и «V» были попарно неотличимы и использовались одна вместо другой.

Таблица 15. Английский алфавит и кодировка во времена Бэкона

AAAAA	g	AABBA	n	ABBAA	t	BAABA
AAAAB	h	AABBB	o	ABBAB	u + v	BAABB
AAABA	i + j	ABAAA	p	ABBBA	w	BABAA
AAABB	k	ABAAB	q	ABBBB	x	BABAB
AABAA	l	ABABA	r	BAAAA	y	BABBA
AABAB	m	ABABB	s	BAAAB	z	BABBB

Вариант шифра Бэкона, использующий современный английский алфавит:

Таблица 16. Современный английский алфавит и кодировка

a	AAAAA	g	AABBA	m	ABBAA	s	BAABA	y	BBAAA
b	AAAAB	h	AABBB	n	ABBAB	t	BAABB	z	BBAAB
c	AAABA	i	ABAAA	o	ABBBA	u	BABAA		
d	AAABB	j	ABAAB	p	ABBBB	v	BABAB		
e	AABAA	k	ABABA	q	BAAAA	w	BABBA		
f	AABAB	l	ABABB	r	BAAAB	x	BABBB		

Способы сокрытия сообщения

Способ 1

Его предложил сам Фрэнсис Бэкон. Пусть в тексте используются два различных типографских шрифта: один для кодирования символа «A», другой — для «B». В простейшем случае можно печатать курсивные буквы вместо «A» и прямые - вместо «B». Например, фамилия:

B *a c o* n

B A A A B

будет соответствовать букве «S».

Способ 2

Обычная фраза:

вот и Наступила ДолГОжДаННая зима

Текст разбивается по 5 букв, пробелы удаляются:

вотиН аступ илаДо лГОжД аННая зима

Большим буквам в тексте ставятся в соответствие символ «B», а маленьким — «A»[7]. Получается сообщение вида:

AAAAB AAAAA AAABA ABBAB ABBAA

При использовании первого варианта кодирования алфавита получается секретное сообщение:

bacon

Способ 3

Теперь правило следующее: буквы алфавита с «A» по «M» соответствуют «A», а буквы с «N» по «Z» — символу «B»[7]. Секретное сообщение шифруется так:

I set the chair right.

A BAB BAA AAAAB BAAAB

Последовательность символов разбивается на части по 5 штук:

ABABB AAAAA ABBAA AB

Последние 2 символа отбрасываются, тогда по первому варианту кодирования алфавита получается секретное сообщение:

man

Такой способ шифрования более сложный, чем второй, и зашифрованное сообщение не так очевидно.

Способ 4

Теперь рассмотрим следующее правило: буквам стоящим на нечётных местах в алфавите (a, c, e…) будет сопоставляться символ «A», на чётных позициях (b, d, f…) — «B».

При таком способе сокрытия текста слово:

knife

ABABA

будет кодировать букву «K».

Вариант шифра Бэкона, использующий современный русский алфавит

Таблица 17. Шифр Бэкона для русского алфавита

№	Буква		№	Буква		№	Буква	
1	А	AAAAAB	12	К	AABBAA	23	Х	ABABBB
2	Б	AAAABA	13	Л	AABBAB	24	Ц	ABBAAA
3	В	AAAABB	14	М	AABBBA	25	Ч	ABBAAB
4	Г	AAABAA	15	Н	AABBBB	26	Ш	ABBABA
5	Д	AAABAB	16	О	ABAAAA	27	Щ	ABBABB
6	Е	AAABBA	17	П	ABAAAB	28	Ъ	ABBBAA
7	Ё	AAABBB	18	Р	ABAABA	29	Ы	ABBBAB
8	Ж	AABAAA	19	С	ABAABB	30	Ь	ABBBBA
9	З	AABAAB	20	Т	ABABAA	31	Э	ABBBBB
10	И	AABABA	21	У	ABABAB	32	Ю	BAAAAA
11	Й	AABABB	22	Ф	ABABBA	33	Я	BAAAAB
0			AAAAAA			. (точка)		

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Исходное сообщение	Иркутск
Ключ	Способ 1

Вариант 2

Исходное сообщение	Вологда
Ключ	Способ 2

Вариант 3

Исходное сообщение	Воронеж
Ключ	Способ 3

Вариант 4

Исходное сообщение	Иваново
Ключ	Способ 1

Вариант 5

Исходное сообщение	Саратов
Ключ	Способ 2

Вариант 6

Исходное сообщение	Белгород
Ключ	Способ 3

Вариант 7

Исходное сообщение	Кемерово
Ключ	Способ 1

Вариант 8

Исходное сообщение	Мурманск
Ключ	Способ 2

Вариант 9

Исходное сообщение	Оренбург
Ключ	Способ 3

Вариант 10

Исходное сообщение	Смоленск
Ключ	Способ 1

Шифр Гронсфельда

Этот сложный шифр подстановки, известный как шифр Гронсфельда, является видоизменением шифра Цезаря с применением числового ключа. При этом под буквами открытого текста записываются цифры ключа. Если ключ оказывается короче сообщения, его запись циклически повторяется. Зашифрованный текст получается аналогично шифру Цезаря, но отсчет по

алфавиту ведётся не по третьей букве (как в шифре Цезаря), а выбирается та буква, которая смещена на соответствующую цифру ключа. Таблица для смещения буквы исходного сообщения по цифре ключа приведена ниже.

	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
0	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	0
1	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	1
2	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	2
3	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	3
4	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	4
5	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	5
6	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	6
7	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	7
8	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	8
9	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	9

Рисунок 18. Шифр Гронсфельда

Пример
Сообщение: МИРЭА
Ключ: 152 15
Шифротекст ННТЮЕ.

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	РХЖЦОЕЕДЖТЁРЮ
Ключ	15270

Вариант 2

Зашифрованное сообщение	НЦЙПЧСИСАЩЛЕ
Ключ	36105

Вариант 3

Зашифрованное сообщение	ЙУУОЧЫЗРЭЗ
Ключ	73514

Вариант 4

Зашифрованное сообщение	ЧФЫЕНУФ
Ключ	62819

Вариант 5

Зашифрованное сообщение	ЫСШТПХНОУУ
Ключ	39421

Вариант 6

Зашифрованное сообщение	ДФЛКЩТСРБ
Ключ	41827

Вариант 7

Зашифрованное сообщение	ОЁЦЁМФЁ
Ключ	46218

Вариант 8

Зашифрованное сообщение	ГУЗФЩЛЪС
Ключ	38569

Вариант 9

Зашифрованное сообщение	ЯКЧСУИВРЙЙ
Ключ	72315

Вариант 10

Зашифрованное сообщение	ЦСХВЩЙРПЁ
Ключ	53710